Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of Lenovo (United States) Inc., File No. 152 3134

The Federal Trade Commission has accepted, subject to final approval, an agreement containing a consent order from Lenovo (United States), Inc. ("Lenovo").

The proposed consent order has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission again will review the agreement and the comments received and will decide whether it should withdraw from the agreement or make final the agreement's proposed order.

This matter involves Lenovo, one of the world's largest personal computer manufacturers, and its preinstallation on certain consumer laptops of VisualDiscovery, an ad-injecting software developed by Superfish, Inc. and customized for Lenovo. VisualDiscovery injected pop-up ads of similar-looking products sold by Superfish's retail partners whenever a consumer's cursor hovered over a product image while browsing on a shopping website. For example, when a consumer's cursor hovered over an image of owl-shaped pendants on a shopping website like amazon.com, VisualDiscovery would show the user pop-up ads of similar-looking owl pendants. To do so, VisualDiscovery acted as a "man-in-the-middle" between consumers' browsers and the websites they visited, including encrypted https:// websites. This man-in-the-middle technique allowed VisualDiscovery to see all of a consumer's sensitive personal information that was transmitted on the Internet, such as login credentials, Social Security numbers, financial account information, medical information, and email communications. VisualDiscovery then collected, transmitted to Superfish servers, and stored a more limited subset of user information, including the website addresses visited by consumers, consumers' IP addresses, and a unique identifier assigned by Superfish to each user's laptop. Superfish had the ability to collect additional information from Lenovo users through VisualDiscovery at any time.

To facilitate its injection of pop-up ads into encrypted https:// websites, VisualDiscovery installed a self-signed root certificate in the laptop's operating system. This allowed VisualDiscovery to replace the digital certificates for https:// websites with VisualDiscovery's own certificates for those websites and caused consumers' browsers to automatically trust the VisualDiscovery-signed certificates. Digital certificates are part of the Transport Layer Security (TLS) protocol that, when properly validated, serve as proof that consumers are communicating with the authentic https:// website and not an imposter.

As alleged in the complaint, VisualDiscovery's substitution of digital certificates for https:// websites with its own certificates for those websites created two significant security vulnerabilities. First, VisualDiscovery did not adequately verify that websites' digital certificates were valid before replacing them with its own certificates, which were automatically trusted by consumers' browsers. This rendered a critical browser security function useless

because browsers would no longer warn consumers that their connections were untrusted when they visited potentially spoofed or malicious websites with invalid digital certificates.

The complaint also alleges that VisualDiscovery created a second security vulnerability by using a self-signed root certificate with the same private encryption key and the same easy-to-crack password on every laptop rather than employing private keys unique to each laptop. This violated basic encryption key management principles because attackers who cracked the simple password on one consumer's laptop could then target every affected Lenovo user with man-in-the-middle attacks that could intercept consumers' electronic communications with any website, including those for financial institutions and medical providers. Such attacks would provide attackers with unauthorized access to consumers' sensitive personal information, such as Social Security numbers, financial account numbers, login credentials, medical information, and email communications. This vulnerability also made it easier for attackers to deceive consumers into downloading malware onto any affected Lenovo laptop. The risk that this vulnerability would be exploited increased after February 19, 2015, when news of these vulnerabilities became public and bloggers posted instructions on how the vulnerabilities could be exploited.

The complaint alleges that Lenovo failed to discover these significant security vulnerabilities because it failed to take reasonable measures to assess and address security risks created by third-party software it preinstalled on its laptops. Specifically, Lenovo allegedly:

- failed to adopt and implement written data security policies applicable to third-party preinstalled software;
- failed to adequately assess the data security risks of third-party software prior to preinstallation;
- failed to request or review any information prior to preinstallation about Superfish's data security policies, procedures or practices;
- failed to require Superfish by contract to adopt and implement reasonable data security measures;
- failed to assess VisualDiscovery's compliance with reasonable data security standards; and
- failed to provide adequate data security training for employees responsible for testing third-party software.

The complaint alleges that Lenovo's failure was an unfair act that caused or was likely to cause substantial consumer injury that consumers could not reasonably avoid, and that there were no countervailing benefits to consumers or competition.

The Commission's complaint also alleges that Lenovo failed to make adequate disclosures about VisualDiscovery to consumers. Lenovo did not disclose to consumers that it had preinstalled VisualDiscovery prior to purchase, and the software had limited visibility on the consumer's laptop. Lenovo only disclosed VisualDiscovery through a one-time pop-up window the first time consumers visited a shopping website that stated,

> Explore shopping with VisualDiscovery: Your browser is enabled with VisualDiscovery which lets you discover visually similar products and best prices while you shop.

The pop-up window contained a small opt-out link at the bottom of the pop-up that was easy for consumers to miss. If a consumer clicked on the pop-up's 'x' close button, or anywhere else on the screen, the consumer was opted in to the software.

The complaint alleges that this pop-up window's disclosures were inadequate and violated Section 5 of the FTC Act by failing to disclose, or failing to disclose adequately, that VisualDiscovery would act as a man-in-the-middle between consumers and all the websites they visited, including encrypted https:// websites, and collect and transmit certain consumer Internet browsing data to Superfish. These facts would be material to consumers' decisions whether or not to use VisualDiscovery.

The complaint also alleges that Lenovo's preinstallation of the ad-injecting software that, without adequate notice or informed consent, acted as a man-in-the-middle between consumers and all the websites they visited, including encrypted https:// websites, and collected and transmitted certain consumer Internet browsing data to Superfish was an unfair act that caused or was likely to cause substantial injury to consumers, and that was not offset by countervailing benefits to consumers or competition and was not reasonably avoidable by consumers.

The proposed consent order contains provisions designed to prevent Lenovo from engaging in similar acts and practices in the future.

Part I of the proposed order prohibits Lenovo from making any misrepresentations about certain preinstalled software on its personal computers.

Part II of the proposed order requires Lenovo to obtain a consumer's affirmative express consent, with certain limited exceptions, prior to any preinstalled software a) injecting advertisements into a consumer's Internet browsing session, or b) transmitting, or causing to transmit, the consumer's personal information to any person or entity other than the consumer. Lenovo must also provide instructions for how consumers can revoke their consent to the software's operation by providing a reasonable and effective means for consumers to opt out, disable or remove the software.

Parts III and IV of the proposed order require Lenovo to implement a mandated software security program that is reasonably designed to address security risks in software preinstalled on its personal computers, and undergo biennial software security assessments of its mandated software security program by a third party.

Parts V through IX of the proposed order are standard reporting and compliance provisions. Part V requires dissemination of the order now and in the future to all current and future principals,

officers, directors, and managers, and to persons with managerial or supervisory responsibilities relating to Parts I – IV of the order. Part VI mandates that Lenovo submit a compliance report to the FTC one year after issuance, and then notices, as the order specifies, thereafter. Parts VII and VIII requires Lenovo to retain documents relating to its compliance with the order for a five-year period, and to provide such additional information or documents necessary for the Commission to monitor compliance. Part IX states that the Order will remain in effect for 20 years.

The purpose of this analysis is to aid public comment on the proposed order. It is not intended to constitute an official interpretation of the complaint or proposed order, or to modify in any way the proposed order's terms.